

# CERTPARK



## QUESTION & ANSWER



CERTPARK.COM

Accurate Study Guides,  
High Passing Rate!  
provides update  
free of charge  
in one year!



**Exam** : **CIPM**

**Title** : Certified Information Privacy  
Manager (CIPM)

**Version** : DEMO

1.What is the best way to understand the location, use and importance of personal data within an organization?

- A. By analyzing the data inventory.
- B. By testing the security of data systems.
- C. By evaluating methods for collecting data.
- D. By interviewing employees tasked with data entry.

**Answer: C**

**Explanation:**

The best way to understand the location, use and importance of personal data within an organization is by evaluating methods for collecting data. This will help to identify the sources, purposes, and categories of data that the organization processes, as well as the data flows and transfers within and outside the organization. By doing so, the organization can assess the risks and opportunities associated with data processing and design appropriate privacy policies and controls.

Reference: [IAPP CIPM Study Guide], page 29-30; [Data Inventory]

2.What are you doing if you succumb to "overgeneralization" when analyzing data from metrics?

- A. Using data that is too broad to capture specific meanings.
- B. Possessing too many types of data to perform a valid analysis.
- C. Using limited data in an attempt to support broad conclusions.
- D. Trying to use several measurements to gauge one aspect of a program.

**Answer: A**

**Explanation:**

If you succumb to "overgeneralization" when analyzing data from metrics, you are using data that is too broad to capture specific meanings. For example, if you use a single metric such as "number of complaints" to measure customer satisfaction, you are ignoring other factors that may affect customer satisfaction such as quality of service, responsiveness, or loyalty. You are also assuming that all complaints are equally valid and important, which may not be the case. To avoid overgeneralization, you should use multiple metrics that are relevant, specific, and measurable for your objectives.

Reference: [IAPP CIPM Study Guide], page 59-60; [Avoiding Overgeneralization in Data Analysis]

3.In addition to regulatory requirements and business practices, what important factors must a global privacy strategy consider?

- A. Monetary exchange.
- B. Geographic features.
- C. Political history.
- D. Cultural norms.

**Answer: D**

**Explanation:**

In addition to regulatory requirements and business practices, an important factor that a global privacy strategy must consider is cultural norms. Different cultures may have different expectations and preferences regarding privacy, such as what constitutes personal information, how consent is obtained and expressed, how data is used and shared, and how privacy rights are enforced. A global privacy strategy should respect and accommodate these cultural differences and ensure that the organization's privacy practices are transparent, fair, and consistent across different regions.

Reference: [IAPP CIPM Study Guide], page 81-82; [Cultural Differences in Privacy Expectations]

4. What have experts identified as an important trend in privacy program development?

- A. The narrowing of regulatory definitions of personal information.
- B. The rollback of ambitious programs due to budgetary restraints.
- C. The movement beyond crisis management to proactive prevention.
- D. The stabilization of programs as the pace of new legal mandates slows.

**Answer: C**

**Explanation:**

An important trend in privacy program development is the movement beyond crisis management to proactive prevention. This means that instead of reacting to privacy breaches or incidents after they occur, organizations are taking steps to prevent them from happening in the first place. This involves implementing privacy by design principles, conducting privacy impact assessments, adopting privacy-enhancing technologies, training staff on privacy awareness and best practices, and monitoring compliance and performance. By doing so, organizations can reduce risks, costs, and reputational damage associated with privacy violations.

Reference: [IAPP CIPM Study Guide], page 93-94; [Moving from Crisis Management to Proactive Prevention]

## 5. SCENARIO

Please use the following to answer the next QUESTION:

Manasa is a product manager at Omnipresent Omnimedia, where she is responsible for leading the development of the company's flagship product, the Handy Helper. The Handy Helper is an application that can be used in the home to manage family calendars, do online shopping, and schedule doctor appointments. After having had a successful launch in the United States, the Handy Helper is about to be made available for purchase worldwide.

The packaging and user guide for the Handy Helper indicate that it is a "privacy friendly" product suitable for the whole family, including children, but does not provide any further detail or privacy notice. In order to use the application, a family creates a single account, and the primary user has access to all information about the other users. Upon start up, the primary user must check a box consenting to receive marketing emails from Omnipresent Omnimedia and selected marketing partners in order to be able to use the application.

Sanjay, the head of privacy at Omnipresent Omnimedia, was working on an agreement with a European distributor of Handy Helper when he fielded many Questions about the product from the distributor. Sanjay needed to look more closely at the product in order to be able to answer the Questions as he was not involved in the product development process.

In speaking with the product team, he learned that the Handy Helper collected and stored all of a user's sensitive medical information for the medical appointment scheduler. In fact, all of the user's information is stored by Handy Helper for the additional purpose of creating additional products and to analyze usage of the product. This data is all stored in the cloud and is encrypted both during transmission and at rest.

Consistent with the CEO's philosophy that great new product ideas can come from anyone, all Omnipresent Omnimedia employees have access to user data under a program called Eureka. Omnipresent Omnimedia is hoping that at some point in the future, the data will reveal insights that could

be used to create a fully automated application that runs on artificial intelligence, but as of yet, Eureka is not well-defined and is considered a long-term goal.

What step in the system development process did Manasa skip?

- A. Obtain express written consent from users of the Handy Helper regarding marketing.
- B. Work with Sanjay to review any necessary privacy requirements to be built into the product.
- C. Certify that the Handy Helper meets the requirements of the EU-US Privacy Shield Framework.
- D. Build the artificial intelligence feature so that users would not have to input sensitive information into the Handy Helper.

**Answer:** B

**Explanation:**

Manasa skipped the step of working with Sanjay to review any necessary privacy requirements to be built into the product. This step is part of the system analysis phase, which is less theoretical and focuses more on practical application<sup>1</sup> By working with Sanjay, Manasa could have identified the legal and ethical obligations that Omnipresent Omnimedia has to protect the privacy of its users, especially in different jurisdictions. She could have also incorporated privacy by design principles, such as data minimization, purpose limitation, and user consent, into the product development process<sup>2</sup> This would have helped to avoid potential privacy risks and violations that could harm the reputation and trust of the company and its customers.

Reference: 1: 7 Phases of the System Development Life Cycle (With Tips); 2: [Privacy by Design: The 7 Foundational Principles]